Operating Instructions (For User Authentication)

e-STUDIO191F
The following trademarks and registered trademarks are used throughout this manual:

Microsoft, Windows, Windows Server, Windows Vista, Excel, PowerPoint, Outlook & Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the USA and other countries.
Adobe, Acrobat Reader & Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated.
All other trademarks identified herein are the property of their respective owners.

© 2011 TOSHIBA TEC CORPORATION All rights reserved
Unauthorized copying and distribution is a violation of law.

The contents of these Operating Instructions are subject to change without notice.
Table of Contents

General Description ............................................... 4
  ■ User Authentication .................................................... 4
  ■ Job Tracking ............................................................... 5
  ■ RightFax Server .......................................................... 6

Using Machine (for User) ........................................ 8
  ■ Login Procedure (Using Copy/Fax/Scanner/Printer) .......... 8
  ■ Sending a Document via RightFax ............................... 10

Setting Machine .................................................. 11
  ■ Authentication Setting ................................................. 11
  ■ Registration of Domain Name ........................................ 14
  ■ ID Timeout Setting ....................................................... 15
  ■ Auto Reset Time Setting .............................................. 16
  ■ Logon Attempts Setting ................................................ 17
  ■ Lockout Time Setting ................................................... 18
  ■ Authentication Method Setting ...................................... 19
  ■ Job Tracking Setting .................................................... 20
  ■ RightFax Server Setting ................................................ 22

Appendix ............................................................. 24
  ■ Administrator Login ................................................... 24
  ■ Administrator Name & Password .................................. 25
  ■ Description of Job Tracking Notice ............................... 26
User Authentication

The User Authentication is a function to use devices under the management of a Windows® server. Users must be authenticated before using the functions of the machine (copying, faxing, scanning, and printing). The supported authentication protocol is NTLM v2.

Windows Server
- Windows 2000 Server®
- Windows Server® 2003
- Windows Vista®
- Windows Server® 2008 or
- Windows® 7

TOSHIBA Device

Users
- Users login to the TOSHIBA machine using their Windows account (user name and password).

System administrator
- The system administrator can manage user accounts by using the Windows Server.
- User authentication can be set independently for each function (copying, faxing, scanning, and printing).

Note
1. NTLM authentication is a user authentication protocol used in the Windows NT family of operating systems.
   NTLM uses a challenge/response method, and operates in such a way that the password is not sent across the network in clear text. In Windows 2000, this protocol can also be used to maintain compatibility between client and server.
**Job Tracking**

While using User Authentication, it is also possible to use the Job Tracking function as well. The Job Tracking function allows the system administrator to receive a machine usage log and send/receive log via Email. The Email to the administrator includes the name of the machine user, destination, and communication time, together with the image of the document that was sent or received.

![Diagram showing the connection between TOSHIBA Device, PSTN, Windows Server, System Administrator, and LAN](image)

1. Fax Transmission and Reception via PSTN.
2. Email Transmission to an Internet Fax, or a PC.
3. Reception from an Internet Fax, or a PC.

**NOTE**

1. When the Job Tracking function is enabled, the following functions are not available.
   - Fax Forward (Fax Parameter No. 54)

For details, refer to the Operating Instructions.
RightFax Server

By enabling the RightFax Server function, all the faxes will be sent via the RightFax Server. All the fax logs can be easily managed by a single server.

When using it with the User Authentication function, it will increase the security by controlling the usage and identifying the users.

- The fax document to be sent is passed to the RightFax server via Email.
- A user who sends a fax from a TOSHIBA machine can receive a send confirmation report on the PC from the RightFax server.

NOTE

1. When the RightFax function is enabled, the following functions are not available.
   - Deferred Polling
   - Sub-Address Transmission
   - LAN Relay Transmission
   - Polling
   - Fax Cover Sheet
   - Direct Transmission

   The document(s) is always stored into memory when sending the document(s).

   For details, refer to the Operating Instructions.

2. Requires RightFax Ver. 8.0 or later.
Login Procedure (Using Copy/Fax/Scanner/Printer)

Users must enter the login name and the password before using any devices which have the User Authentication function enabled. Authentication is performed using the user's Windows account.

1. The User Authentication function becomes enabled after you perform "Authentication Setting" and "Registration of Domain Name" (See pages 11 to 14). The control panel display changes from the standby message to the login prompt.
2. Make sure that the Host Name has been set properly. For details, refer to the Operating Instructions.

1. A login prompt appears if user authentication is enabled.

   Note:
   User authentication can be set independently for each function (copying, faxing, scanning, and printing).
   If user authentication is disabled for the fax function, the control panel displays the standby message and the login prompt only appears when a function that requires authentication is selected.

2. Enter your user name, and then press SET. (Up to 40 characters)
   The user name is NOT case-sensitive.
   Ex: toshiba

   Note:
   Accepts following characters.
   , & ( ) : / _ . * + % = \* $ ; < > ? [ ] ^ ` { | } * # and alphanumeric characters

3. Enter your password, and then press SET. (Up to 40 characters)
   The password is case-sensitive.
   Ex: toshiba

   Note:
   Accepts following characters.
   , & ( ) : / _ . * + % = \* $ ; < > ? [ ] ^ ` { | } * # and alphanumeric characters

4. Press ▲ or ▼ to select the domain, and then press SET.
   Ex: TOSHIBA01
5 This completes the authentication.

After completing the authentication, you can use the selected function (copying, faxing, scanning, or printing).

**Note:**
- If the authentication fails, one of the following messages may appear.

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGIN FAILED</td>
<td>The login failed. Check your user name and password. Check whether the Date and Time is set properly.</td>
</tr>
<tr>
<td>LOGON ATTEMPTS EXCEEDED</td>
<td>The system has been locked because the permitted number of login attempts has been exceeded. Please contact the system administrator.</td>
</tr>
<tr>
<td>CONNECTION FAILED</td>
<td>Unable to connect to the authentication server. Please contact the system administrator.</td>
</tr>
<tr>
<td>PROTOCOL ERROR</td>
<td>Unable to connect to the authentication server. Please contact the system administrator.</td>
</tr>
<tr>
<td>SERVER NOT FOUND</td>
<td>Unable to locate the authentication server. Check whether the DNS Domain Name is set properly (see page 14). Check whether the Internet Parameters are set properly.</td>
</tr>
</tbody>
</table>
  - IP Address
  - Subnet Mask
  - Default Gateway IP Address
  - DNS Server Addresses

- Authentication is cancelled if no operation is performed on the machine within a certain period of time after authentication is completed. In this case, you need to perform user authentication again before using the machine. The system administrator can specify the ID Timeout Period. See “ID Timeout Setting” on page 15 for details.
- The system administrator can specify whether authentication is required independently for each machine function (copying, faxing, scanning, and printing). See “Authentication Setting” on page 11 for details.
Sending a Document via RightFax

When the RightFax server is used to send a fax, the following details are entered in the recipient (TO) field and sender (FROM) field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipient</td>
<td>Station Name registered for One-Touch or ABBR. dialing. If manual number dialing is used, you can enter the user name from the control panel.</td>
</tr>
<tr>
<td>Sender</td>
<td><strong>When the user authentication is not enabled</strong></td>
</tr>
<tr>
<td></td>
<td>Logo and Email Address of this device.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>Name and Email Address selected with the <strong>Sender Selection</strong> function.</td>
</tr>
<tr>
<td></td>
<td><strong>When the user authentication is enabled</strong></td>
</tr>
<tr>
<td></td>
<td>Name of the authenticated user registered with the Windows Server.</td>
</tr>
</tbody>
</table>

**Note:**
- RightFax Server is available in certain countries only.

1. Login, and then set document(s) on the ADF.

   **Note:**
   If you need to login, see "Login Procedure" on page 8 for details.

2. Specify the recipient.

   Ex: 5551234

   **Note:**
   Quick Name Search dialing, One-Touch/ABBR. dialing, and Directory Search dialing can be used to specify the recipient. For details, refer to the Operating Instructions.

3. Press **START** to scan the document, and then start sending.

   If you press **SET** instead of **START** when using manual number dialing, you can enter the recipient's name. (Up to 15 characters). Continue following operation.

4. Enter the name, and then press **SET**.

5. When you press **START**, the machine scans the document and starts sending.
Authentication Setting

The system administrator can enable/disable the user authentication for each function (copying, faxing, scanning, and printing).

1. Press FUNCTION 7 4 SET.

2. Enter Operator’s ID Code, and then SET.

3. Press 1 2 6, and then press SET.

4. Select the function where authentication is required.

   - 1 SET: Selects the copy function.
   - 2 SET: Selects the fax function.
   - 3 SET: Selects the printer function.
   - 4 SET: Selects the scanner function.

   **Note:**
   *The Sender Selection feature is not enabled if the fax function is set to require user authentication.*
   *For details, refer to the Operating Instructions.*

5. Select "VALID" to use authentication or "INVALID" to disable authentication.

   - 1 SET: Disables authentication.
   - 2 SET: Enables authentication.

   When user authentication is enabled for the first time, you also need to specify the time zone, system administrator’s name, and password.

Continued on the next page...
Specify the time zone, the system administrator name, and password.

Press or to select the time zone.

Press SET.

Enter the administrator name you wish to use, and then press SET.

Enter the administrator password, and then press SET.

Note: The administrator name and password set here are required in subsequent setup operations (see page 25). Please keep them in a safe place.
7 The next function appears (return to step 4).
   To continue with the setup, press [SET].

8 Press [STOP] to return to standby.
Registration of Domain Name

This sets the NetBIOS domain names and DNS suffix to use for user authentication.

1. Press [FUNCTION] ① ① SET.

2. Enter Operator's ID Code, and then SET.

3. Press ▲ and select "AUTH DOMAIN".

4. Press SET.

5. A prompt appears to set the NetBIOS domain names.
   You can set up to 10 domain names. Press ▲ or ▼ to select the entry number ("01" to "10").

6. Enter the NetBIOS domain name, and then press SET. (Up to 15 characters)

7. Enter the DNS domain name, and then press SET. (Up to 60 characters)

8. The next number entry field appears (return to step 5).
   Enter the next domain name if required.

9. Press STOP to return to standby.
ID Timeout Setting

If the ID Timeout Setting is set to "AUTO RESET TIME", authentication is cancelled if no operation is performed on the machine for a specified time period after performing authentication. The ID timeout period is set by the "AUTO RESET TIME Setting" on page 16.

Note:
When the User Authentication function is enabled, you must login to the machine to change settings. See the following sections for details about how to login.
See "Administrator Login" on page 24 for Logging in as the system administrator.
See "Login Procedure" on page 8 for Logging in as a user.

1 Login to the machine, and then press [FUNCTION 7 4 SET].
2 Enter Operator’s ID Code, and then [SET].
3 Press 1 2 7, and then press [SET].
4 Select the ID Timeout setting.
   1 [SET] : (AUTO RESET TIME) An authenticated user will be logged out if no operation is performed on the machine for a specified time after performing authentication.
   2 [SET] : (AFTER EVERY JOB) An authenticated user will be logged out when the performing operation is completed.
5 Press [STOP] to return to standby.
Auto Reset Time Setting

This sets the ID timeout period when "AUTO RESET TIME" is selected for the ID Timeout Setting.

**Note:**
When the User Authentication function is enabled, you must login to the machine to change settings. See the following sections for details about how to login.
See "Administrator Login" on page 24 for Logging in as the system administrator.
See "Login Procedure" on page 8 for Logging in as a user.

1. Login to the machine, and then press [FUNCTION] 7 4 [SET].

2. Enter Operator's ID Code, and then [SET].

3. Press 1 2 1, and then press [SET].

4. Select the timeout for canceling authentication.
   - 1 [SET]: (OFF) If "OFF" is selected, the authentication is not reset, regardless of the elapsed time.
   - 2 [SET]: 30 seconds
   - 3 [SET]: 1 minute
   - 4 [SET]: 2 minutes
   - 5 [SET]: 3 minutes
   - 6 [SET]: 4 minutes

5. Press [STOP] to return to standby.
Logon Attempts Setting

The system is locked if the permitted number of logon attempts is exceeded during the user authentication. This sets the permitted number of logon attempts.

Note:
When the User Authentication function is enabled, you must login to the machine to change settings. See the following sections for details about how to login.
See "Administrator Login" on page 24 for Logging in as the system administrator.
See "Login Procedure" on page 8 for Logging in as a user.

1. Login to the machine, and then press FUNCTION 7 4 SET.

2. Enter Operator's ID Code, and then SET.

3. Press 1 2 1, and then press SET.

4. Enter the number of logon attempts (0 to 9), and then press SET.

   Unlimited login attempts is allowed if you set 0.

5. Press STOP to return to standby.
### Lockout Time Setting

This sets the time period (minutes) for the system lockout when the permitted number of logon attempts is exceeded during the user authentication. Wait for the Lockout Time period to lapse before you are permitted to logon to user authentication.

1. Login to the machine, and press `FUNCTION 7 4 SET`.

2. Enter Operator’s ID Code, and then `SET`.

3. Press `1 2 4`, and then `SET`.

4. Enter the number of logon attempts (1 to 60), and then press `SET`.

5. Press `STOP` to return to standby.
Authentication Method Setting

This specifies which authentication method to use by the User Authentication function.

Note:
When the User Authentication function is enabled, you must login to the machine to change settings. See the following sections for details about how to login.
See "Administrator Login" on page 24 for Logging in as the system administrator.
See "Login Procedure" on page 8 for Logging in as a user.

1  Login to the machine, and then press FUNCTION 7 4  SET.

2  Enter Operator's ID Code, and then SET.

3  1 2 3, and then press SET.

4  Select the authentication method.
   1 SET : Selects CLEAR TEXT.
   2 SET : Selects NTLM.

5  Press STOP to return to standby.
Job Tracking Setting

This enables or disables Job Tracking. If Job Tracking is enabled, also set the type of log to record and the Email address to which it is to be sent.

Note:
- Before performing this setup, you first need to register the destination Email address for the log in the Auto Dialers. Furthermore, change the setting of the Fax Forward (Fax Parameter No. 54, FAX FORWARD) parameter to Invalid.
- Set the POP Parameters so as to receive the emails automatically when using the Job Tracking function. Otherwise, your machine cannot receive any emails.
- Make sure that the Fax Parameters are NOT set as below.
  Auto POP Receive (Fax Parameter No. 147) : Invalid
  POP Timer (Fax Parameter No. 146) : 0 minute
- When the User Authentication function is enabled, you must login to the machine to change settings. See the following sections for details about how to login.
  See "Administrator Login" on page 24 for Logging in as the system administrator.
  See "Login Procedure" on page 8 for Logging in as a user.
- The Job Tracking setting is cleared if the Authentication Setting of all functions is changed to Invalid.

1. Login to the machine, and then press **FUNCTION** ② ④ **SET**.  
   
2. Enter Operator’s ID Code, and then **SET**.  
   
3. Press ① ② ①, and then **SET**.  
   
4. Enable ("VALID") or disable ("INVALID") the Job Tracking function.  
   ① **SET** : Disables Job Tracking.  
   ② **SET** : Enables Job Tracking.  
   If you selected ② (VALID), next specify the type of log to record and the Email address to which it is to be sent.  

5. Select the type of log to record.  
   ① **SET** : (TX) Records sending only.  
   ② **SET** : (RX) Records receiving only.  
   ③ **SET** : (TX&RX) Records sending and receiving.  

6. A prompt appears for entering the destination Email address.  

7. Select the destination Email address to which to send the log from the addresses previously set in the Auto Dialers.
8. SET twice. (In case the Fax Parameter No. 119, Qwerty Keyboard, is set to One-Touch, press SET once.)

9. Select the printout method for the received document(s). This parameter is only enabled if the RX or TX&RX is selected on the step 5.
   ① SET : (INC) Prints only if the log was unable to be sent to the specified destination.
   ② SET : (ON) Always prints.

10. Press STOP to return to standby.
Setting Machine

RightFax Server Setting

This enables or disables the RightFax server.

**Note:**
- When the User Authentication function is enabled, you must login to the machine to change settings. See the following sections for details about how to login. See "Administrator Login" on page 24 for Logging in as the system administrator. See "Login Procedure" on page 8 for Logging in as a user.
- RightFax Server is available in certain countries only.
- The machine will generate the Email Address in the format as below, and then send the Email to the RightFax Server.

*Ex: "lfax=5551212/name=Jane/"<rightfax@toshiba.com>*

<table>
<thead>
<tr>
<th>Fax Number</th>
<th>Station Name</th>
<th>Email Address of the RightFax Server</th>
</tr>
</thead>
</table>

1. Login to the machine, and then press **FUNCTION 7 4 SET**.

2. Enter Operator's ID Code, and then **SET**.

3. Press 1 3 2, and then press **SET**.

4. Enable ("VALID") or disable ("INVALID") the RightFax server.

   1. **SET**: Disables the RightFax server.
   2. **SET**: Enables the RightFax server.

   When you enable the RightFax server for the first time, you also need to enter the Email address of the server.

5. A prompt appears for entering the Email address.

6. Enter the Email address of the RightFax server, and then press **SET**.
   (Up to 60 characters)

7. Press **STOP** to return to standby.
Administrator Login

This confirms the system administrator who manages the TOSHIBA machine. After logging in to the machine, the system administrator can set up the authentication function.

**Note:**
*Refer to Authentication Setting (see page 11) for the registration of Administrator’s Name and Password.*

1. The login prompt appears if the user authentication function has been enabled.

2. Enter the administrator name, and then press [SET].
   The administrator name is **NOT** case-sensitive.

3. Enter the password, and then press [SET].
   The password is case-sensitive.

4. Press ▲ or ▼ to select "LOCAL MACHINE", and then press [SET].

5. This completes the authentication.
Administrator Name & Password

The user name and password for the system administrator are established in "Authentication Setting" on page 11 when user authentication is enabled for the first time. Use the following procedure if you subsequently wish to change the system administrator name or password.

**Note:**
You must login to the machine before you can change settings. See the following sections for details about how to login. See "Administrator Login" on page 24 for Logging in as the system administrator. See "Login Procedure" on page 8 for Logging in as a user.

1. Login to the machine, and then press FUNCTION ⑦① SET.

2. Enter Operator’s ID Code, and then SET.

3. Press ▲, and select "ADMINISTRATOR NAME".

4. The currently set administrator name is displayed.

5. Enter the new administrator name, and then press SET.
   The name is NOT case-sensitive.

6. Enter the administrator password, and then press SET.
   The password is case-sensitive.

7. Press STOP to return to standby.
### Description of Job Tracking Notice

#### Table

<table>
<thead>
<tr>
<th>Job Type</th>
<th>Fax Transmission via PSTN</th>
<th>Reception via PSTN</th>
<th>Reception from Internet Fax / PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Sender's Name or Login Name in the User Authentication</td>
<td>Fax: ID Number of the remote station or Sender's ID Unknown (In case the remote station has not registered the ID number.)</td>
<td>FWD: Sender's Email Address</td>
</tr>
<tr>
<td>2.</td>
<td>Transmitted Date and Time</td>
<td>Received Date and Time</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Recipient's Email Address, or Machine's Email Address</td>
<td>Recipient's Email Address (as set in the Job Tracking Setting, see page 20)</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Subject</td>
<td>Default Subject of the machine or specified subject with Subject Line Entry function. If no subject is entered, the following subject is shown instead. <strong>IMAGE from Internet FAX</strong></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Transmitted document(s)</td>
<td>Received document(s)</td>
<td>Received document(s) * Email Body Text is included in the attached file as image.</td>
</tr>
<tr>
<td>6.</td>
<td>Fixed Message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Number of Destination(s)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Transmitted Address(es)</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

---

*An image data in TIFF-F format has been attached to this email. You can view and print this TIFF-F Image Viewer from the following URL addresses:

http://panasonic.co.jp/pcc/en

005.DESTINATION(S):

aggggg@fax.panasonic.com
tttttt@newyork.panasonic.com
cccc@london.panasonic.com
0 001 1234 5670
0 002 1234 5678